FORM PTO-1390 (REV. 11-2000)	U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY 'S DOCKET NUMBER
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		833.1001
		U S APPLICATION NO (If known, see 37 CFR 1 5 **09/720702**

INTERNATIONAL APPLICATION NO. PCT/DE99/01937	INTERNATIONAL FILING DATE 30 June 1999	PRIORITY DATE CLAIMED 30 June 1998

TITLE OF INVENTION Method for Determining the Origin and/or Identifying of Animals or Biological Material.

APPLICANT(S) FOR DO/EO/US
Eberhard Manz

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [x] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.

2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.

3. [X] This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.

4. [ ] The US has been elected by the expiration of 19 months from the priority date (Article 31).

5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [ ] is attached hereto (required only if not communicated by the International Bureau).
   b. [X] has been communicated by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).

6. [X] An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. [X] is attached hereto.
   b. [ ] has been previously submitted under 35 U.S.C. 154(d)(4).

7. [X] Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are attached hereto (required only if not communicated by the International Bureau).
   b. [X] have been communicated by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [ ] have not been made and will not be made.

8. [X] An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).

9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. [ ] An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. [ ] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.

12. [x] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.

13. [x] A FIRST preliminary amendment.

14. [ ] A SECOND or SUBSEQUENT preliminary amendment.

15. [ ] A substitute specification.

16. [ ] A change of power of attorney and/or address letter.

17. [ ] A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.

18. [ ] A second copy of the published international application under 35 U.S.C. 154(d)(4).

19. [ ] A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).

20. [x] Other items or information:
   – English language translation of International Search Report.

U.S. APPLICATION NO (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/720702	PCT/DE99/ 01937	833.1001

CALCULATIONS PTO USE ONLY

21. ☒ The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):

Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO $1000.00

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO $860.00

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO $710.00

International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) $690.00

International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00

ENTER APPROPRIATE BASIC FEE AMOUNT = $ 860.00

Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)). $

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	$
Total claims	41 - 20 =	21	x $18.00	$ 378.00
Independent claims	2 - 3 =	0	x $80.00	$
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ $270.00	$

TOTAL OF ABOVE CALCULATIONS = $ 1238.00

☒ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.   + $ -619.00

SUBTOTAL = $ 619.00

Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). $

TOTAL NATIONAL FEE = $

Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property   + $ 40.00

TOTAL FEES ENCLOSED = $ 659.00

Amount to be refunded:	$
charged:	$

a. ☒ A check in the amount of $ 659.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-0552 A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO

_____
SIGNATURE

Morey B. Wildes
_____
NAME

36,968
_____
REGISTRATION NUMBER

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: :

    Eberhard Manz   :

Serial No.: Unassigned   :

International Appl. No.: PCT/DE99/01937   :

Filed: Herewith   :
                                                         :
For: **METHOD OF DETERMINING THE ORIGIN OF AND/OR
        IDENTIFYING ANIMALS OR BIOLOGICAL MATERIAL**

December 29, 2000

BOX: PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

S I R:

    Preliminary to examination, Applicant hereby amends the above-identified patent

application as follows:

<u>In the Specification:</u>

    On page 1, line 1, please delete "Generatio GmbH u.a.".

    On page 1, line 2, please delete "GM 2238 PCT".

    On page 1, line 6, please add -- <u>Background of the Invention</u> --.

    On page 1a, line 10, please add -- <u>Summary of the Invention</u> --.

    On page 5, line 14, first word, replace "outputting" with -- outputting --.

    On page 12, line 31, please add -- <u>Detailed Description of the Invention</u> --.

Please amend claims 2-31 and 33-41 as follows:

2. (amended)   Method according to [Claim 1, [lacuna] that the] claim 1 further comprising the step of storing predetermined genetic information of one or more animals or of biological material from one or more animals or organisms [is determined and is stored] as reference datasets on a storage medium.

3. (amended)   Method according to Claim 1 [or 2, characterized in that] wherein the data carrier holds further data which have been assigned to the identification data and which relate to the animal to be identified or the biological material to be identified.

4. (amended)   Method according to [Claim [sic] 1 to 3, characterized in that] claim 1 wherein the identification data contain an encrypted message which has been encrypted using a code unambiguously assigned to the individual animal or material.

5. (amended)   Method according to Claim 4, [characterized in that] wherein the encrypted message contains the value of a one-way function (hash), which value is obtained when applying said one-way function to further data which are stored on the data carrier and which relate to the animal to be identified or the biological material to be identified.

6. (amended)   Method according to [one [lacuna] Claims 1 to 5, characterized in that] claim 1 wherein an encrypted message comprises genetic information unambiguously identifying the animal or the material.

7. (amended)   Method according to [one of Claims 3 to 6, characterized in that] claim 3 wherein the identification data comprise encrypted data which relate to the storage location and/or the contents of further data which relate to the animal assigned to the identification data.

8. (amended) Method according to [one of Claims 4 to 7, characterized in that] claim 4 wherein the identification data comprise a message encrypted by a code which is generated in a predetermined unambiguous manner on the basis of a sequence of digits which has been unambiguously assigned to genetic information unambiguously identifying the animal or the material.

9. (amended) Method according to Claim 8, [characterized in that] wherein the sequence of digits forms at least part of the code.

10. (amended) Method according to Claim [8 or 9, characterized in that the key is] 4 wherein the message has been encrypted using a symmetric key.

11. (amended) Method according to Claim [8 or 9, characterized in that] 4 wherein the message has been encrypted on the basis of the private key of an asymmetric pair of keys, with the public key at least in part having a predetermined [connection with] relationship to the genetic information identifying the animal or the material.

12. (amended) Method according to [Claim 11, [lacuna] that] claim 11 wherein the public key comprises a part specific for the animal or the material and a user-specific part.

13. (amended) Method according to [one of Claims 8 to 12, characterized in that] claim 8 wherein the identification data are additionally encrypted using a user-specific key.

14. (amended) Method according to [one of Claims 8 to 13, characterized in that] claim 4 wherein the data on the data carrier, which have been assigned to the identification data, have at least in part been encrypted by a code which is different than the code used for encrypting the identification data.

15. (amended) Method according to [one of Claims 8 to 14, characterized in that] claim 4 wherein the key for decrypting the message contained in the identification data is stored on a

carrier of a chip for communicating with a data processing system via an interface, in particular on a smartcard.

16. (amended) Method according to Claim 15, [characterized in that] wherein the chip has a device for decrypting messages.

17. (amended) Method according to Claim 15 [or 16, characterized in that] wherein the key encoding the message of the identification data is an asymmetric key, the corresponding private key is stored on the chip and the chip has a device for encrypting messages using the private key.

18. (amended) Method according to [one of Claims 15 to 17, characterized in that] claim 15 wherein the chip contains an interface for entering digitized genetic information and a device for verifying the assignment of the stored code to entered digitized genetic information.

19. (amended) Method according to [Claims 18, characterized in that] claim 18 wherein the [comparing] verifying device compares the entered digitized genetic information with a stored value for this information and emits an output signal which indicates whether or not there is a match.

20. (amended) Method according to Claim 18, [characterized in that] wherein, based on the entered digitized genetic information and a stored assignment to the stored key of digitized genetic information unambiguously identifying the animal or the material, the [comparing] verifying device determines a key assigned to the entered information, compares the key determined in this way with the stored key and releases an output signal which indicates whether or not the key determined based on the input matches the stored key.

21. (amended) Method according to [one of Claims 15 to 20, characterized in that] claim 15 wherein the chip holds information identifying one or more users and the decrypting device or

encrypting device is only activated when information stored for identifying a user is entered via an input device.

22. (amended) Method according to [one of Claims 8 to 21, characterized in that] claim 4 wherein the code for decrypting coded information contained in the identification data is stored on a central computer.

23. (amended) Method according to Claim 22, [characterized in that] wherein the computer determines the corresponding key owing to entered or predetermined genetic information and applies said key to the identification data.

24. (amended) Method according to Claim 23, [characterized in that] wherein, after decrypting, the central computer verifies whether predetermined sequences of characters are present in the decrypted text and releases a corresponding output signal to a user.

25. (amended) Method according to Claim 23 [or 24, characterized and that] wherein the information stored on the data carrier and, where appropriate, predetermined genetic information unambiguously identifying the animal or the material are transferred to the central computer.

26. (amended) Method according to [one of Claims 1 to 24, characterized in that] claim 1 wherein the data carrier containing the data related to the animal or the material [is stored on] comprises a portion of a central computer.

27. (amended) Method according to Claim 26, [characterized in that] wherein at least in part the data are access-protected and that access authorization is different for different users of the central computer.

28. (amended) Method according to Claim [27, characterized in that] 26, wherein a proportion of users can access at least part of the stored data only, if a predetermined further user is logged on to the central computer at the same time.

29. (amended) Method according to [one of Claims 26 to 28, characterized in that] claim 26, wherein access to at least part of the stored data is only possible, if the computer has verified access authorization using the data stored on a chip, in particular on a smartcard.

30. (amended) Method according to [one of Claims 27 to 29, characterized in that] claim 26, wherein the computer is set up such that users can write to the stored data related to the animal or the material only together with a digital signature of the user.

31. (amended) Method according to [one of Claims 26 to 30, characterized in that] claim 26 wherein an animal-specific pair of asymmetric keys is used for exchanging a session key for communication of a user with the central computer.

33. (amended) Method according to Claim 32, [characterized in that] wherein the identification data contain an encrypted message which has been encrypted using a key unambiguously assigned to the individual animal.

34. (amended) Method according to Claim 33, [characterized in that] wherein the encrypted message contains the value of a one-way function (hash), which value is obtained when applying said one-way function to further data which are stored on the data carrier and which relate to the animal to be identified or the biological material to be identified.

35. (amended) Method according to [one of Claims 32 to 34, characterized in that] claim 32 wherein the identification data comprise a message encrypted by a code which is generated in a predetermined unambiguous manner on the basis of a sequence of digits which has been unambiguously assigned to genetic information unambiguously identifying the animal or the material.

36. (amended) Method according to Claim 35, [characterized in that] wherein the key is a symmetric key.

37. (amended) Method according to Claim 35, [characterized in that] <u>wherein</u> the information has been encrypted on the basis of an asymmetric pair of keys, with the public key at least in part having a predetermined [connection with] <u>relationship to</u> the genetic information.

38. (amended) Chip carrier for identifying animals, [which is] <u>said chip carrier being</u> set up for communication between a chip on the chip carrier and a computer via an interface, in particular a smartcard, [characterized in that] <u>wherein</u> the chip holds a key which has an unambiguous and predetermined connection with genetic information specific for the individual animal.

39. (amended) Chip carrier according to Claim 38, [characterized in that] <u>wherein</u> the chip has a processor for decrypting messages using the stored key.

40. (amended) [Smartcard] <u>Chip carrier</u> according to [one of Claims 38 or 39 [sic], characterized in that] <u>claim 38 wherein</u> the chip contains an interface for entering digitized genetic information and a device for verifying the assignment of the stored code to entered digitized genetic information.

41. (amended) Computer system for carrying out a method according to [one of Claims 1 to 31, characterized by] <u>claim 1 comprising</u> a central computer having a data carrier which holds identification data which have an unambiguous and predetermined connection with genetic information unambiguously identifying an animal or the biological material.

REMARKS

This application is being amended in order to conform the claims of this application, which was originally filed in Europe, to standard U.S. Patent and Trademark Office practice. No new matter is introduced by these amendments.

Respectfully submitted,

Morey B Wildes
Reg. No. 36,968
Attorney for Applicant

DAVIDSON, DAVIDSON & KAPPEL, LLC
485 Seventh Avenue, 14th Floor
New York, NY 10018
(212) 736-1940

- 8 -

Dr.Eberhard Manz

GM 2238 PCT

Method for proving the pedigree and/or for the
identification of animals or of biological material

The invention relates to a method for proving the
pedigree and/or for the identification of animals or of
biological material. The biological material may be
from animals or from any organisms carrying nucleic
acid as genetic material.

For the registration, purchase or breeding of animals
it is often important to identify an animal
unambiguously, to prove the pedigree of the animal or
to find the owner. In stockbreeding, so-called
studbooks or breeding registers which are kept by
registered breeder organizations are known for proving
the pedigree and performance of breeding animals.
Moreover, animal passports are known which contain
particular data on one animal in each case. These data
include, for example, physical characteristics, results
of blood tests, pedigree or unusual phenotypic
features. Disadvantages here are the small amount of
information, limited data access and difficult data
checking. In the case of generally accessible registers
in particular, there is always the danger of
manipulation by the users.

With biological material from animals or organisms such
as, for example, cell samples or cultures of
microorganisms there is the disadvantage that it is
often impossible to check the identity thereof, since
no characteristic data are available.

The invention solves these problems by a method
according to Claim 1 and/or 32, a chip carrier
according to Claim 38 and/or a computer system
according to Claim 41.

The invention may provide for genetic information of a plurality of animals or of biological material from a plurality of animals or organisms to be determined and stored as reference datasets on a storage medium and for the genetic information or parts of the genetic information of the animal to be identified or of the biological material to be identified being compared with one or more reference datasets.

The invention may also provide for additionally storing characteristics or properties of the animals or the biological material in the reference datasets.

The invention may also provide for the characteristics or properties deducible from the genetic information to be determined and stored in the reference dataset.

The invention may also provide for storing photographic pictures of the animals in the reference datasets.

The invention may also provide for the biological material to be embryos, sperm cells or egg cells from animals.

The invention may also provide for the biological material to be blood samples or tissue samples of animals or cells from cell cultures or microorganisms.

The invention may also provide for storing the reference datasets at a central location.

The invention may also provide for encrypting the reference datasets at the central location.

The invention may also provide for using the particular genetic information as a key. The particular genetic information may be part of the key. It is also possible to provide for the particular genetic information to be

part of an electronic certificate which assigns the key
unambiguously to an individual animal unambiguously
specified by said information and which has been issued
by a certification authority. The form of such a
certificate may be based substantially on the form of a
certificate which is issued for authentication of a
public key in accordance with the Digital Signature
Act. It contains at least said genetic information
which allows unambiguous assignment to an individual
animal, the key assigned to said information or said
individual animal, the public key in the case of
asymmetric encryption, and a digital signature of the
certification authority which certifies that the
assignment is indeed authentic.

The invention may also provide for using a smartcard
for retrieving a reference dataset.

The invention may also provide for entering a password
or other information identifying a user for retrieving
a reference dataset.

The invention may also provide for determining mating
suggestions for breedings using the genetic information
and, where appropriate, further information from the
reference datasets.

The invention may also provide for integrating the
storage medium containing the reference data into an
identity tag carried by the animal.

The invention may also provide for an output device
linked to the storage medium to indicate the genetic
information of the reference datasets in the form of a
histogram.

According to another aspect of the invention, said
invention represents a method for proving the pedigree
and/or for the identification of animals or of

biological material from animals and organisms, which comprises the following steps:

- storing on a data carrier identification data in the form of an encrypted message which has an unambiguous and predetermined connection with genetic information unambiguously identifying an animal or the biological material,

- verifying the identification data with respect to whether said data have the predetermined connection with the genetic information.

The encrypted message generated by the identification data may be assigned to the genetic information by encrypting a message, preferably of particular content, using a code which has been unambiguously assigned to the genetic information and therefore to the individual animal, and/or by the encrypted message containing information, which has an unambiguous and predetermined connection with said genetic information, and, in the simplest case, can be said information itself. Both possibilities may be combined. In the first case, the predetermined connection may be verified by decrypting the message using the key individually assigned to the animal. A successful decryption is proof that the identification data have indeed been assigned to said genetic information. In the second case, a key which is kept at a secure location or which only trustworthy users can access is used to decrypt the encrypted message and the contents of the message are used to verify whether these data or this message belong to a particular animal. Combining both methods leads to double verification of the assignment to the genetic information or to the animal, firstly by successful decryption and secondly by the contents of the decrypted message.

The method according to the invention may in particular comprise the following steps:

- storing on a data carrier genetic information

unambiguously identifying the animal or the material, in conjunction with identification data containing an encrypted message which is unambiguously connected with the genetic

5   information,

- retrieving the identification data through an encrypted message which is unambiguously connected with the genetic information,

- verifying the identification data with respect to

10   whether the genetic information transmitted by the message corresponds to the stored genetic information or whether the stored encrypted message corresponds to the sent encrypted message,

- outputing the genetic information when a match has

15   been detected and therefore the animal or the material has been unambiguously identified.

The invention may also provide for determining the genetic information of one or more animals or of

20 biological material from one or more animals or organisms and for storing said information as reference datasets on a storage medium.

The reference datasets contain the identification data

25 and, where appropriate, further data relating to the particular animal and thus form an electronic register sheet into which the data relating to the animal have been entered and which has been unambiguously assigned to the individual animal through the identification

30 data.

The invention may also provide for storing on the data carrier further data which have been assigned to the identification data and which relate to the animal to

35 be identified or the biological material to be identified. In this context it is in particular possible to provide for the encrypted identification data to contain an indicator or other information about the storage location of said further data so that it is

impossible without knowing the key to change said information, i.e. the assignment of a specific storage area to a particular animal. An attempt to assign a different dataset to a particular animal would

5　therefore be noticed when decrypting the identification data, since either no comprehensible uncoded text is obtained, or the decrypted information about the storage location or about the indicator for the stored data relating to the animal is incorrect.

10　The invention may also provide for the identification data to contain an encrypted message which has been encrypted using a code unambiguously assigned to the individual animal or material.

15　The invention may also provide for the encrypted message to contain the value of a one-way function (hash), which value is obtained when applying said one-way function to further data which are stored on the data carrier and which relate to the animal to be

20　identified or the biological material to be identified.

The invention may also provide for an encrypted message to comprise genetic information unambiguously identifying the animal or the material.

25

The invention may also provide for the identification data to comprise encrypted data which relate to the storage location and/or the contents of further data which relate to the animal assigned to the

30　identification data.

The invention may also provide for the identification data to comprise a message encrypted by a code which is generated in a predetermined unambiguous manner on

35　the basis of a sequence of digits which has been unambiguously assigned to genetic information unambiguously identifying the animal or the material.

The invention may also provide for the sequence of

digits to form at least part of the code.

The invention may also provide for the key to be a symmetrical key.

The invention may also provide for encrypting the information based on an asymmetric pair of keys, with the public key at least in part having a predetermined connection with the genetic information identifying the animal or the material.

The invention may also provide for the public key to comprise a part specific for the animal or the material and a user-specific part.

The invention may also provide for additionally encrypting the identification data using a user-specific key.

The invention may also provide for the data on the data carrier, which have been assigned to the identification data, to have at least in part been encrypted by a code which is different than the code used for encrypting the identification data.

The invention may also provide for the key for decrypting the message contained in the identification data to be stored on a carrier of a chip for communicating with a data processing system via an interface, for example a reading device, in particular on a smartcard.

A chip in accordance with this application is generally to be understood as meaning any electronic or optical component which has at least one memory function and, where appropriate, can also perform logical functions and which has an interface for communicating with a computer system, for example via a reading device or via an optical interface. This should also include in

particular holographic memory units. Apart from the identification data and, where appropriate, an electronic certificate of a certification authority, the chip can also hold further data relating to the animal, for example vaccination data, pedigree data, etc. so that the chip or a carrier on which this chip is installed, for example a smartcard, functions as an animal identity card storing all the data relevant to the animal.

The invention may also provide for the chip to have a device for decrypting messages.

The invention may also provide for the key encoding the message of the identification data to be an asymmetric key, the corresponding private key to be stored on the chip and the chip to have a device for encoding messages using the private key.

The invention may also provide for the chip to contain an interface for entering digitized genetic information and a device for verifying the assignment of the stored code to entered digitized genetic information.

The invention may also provide for the comparing device to compare the entered digitized genetic information with a stored value for this information and to emit an output signal which indicates whether or not there is a match.

The invention may also provide for, based on the entered digitized genetic information and a stored assignment to the stored key of digitized genetic information unambiguously identifying the animal or the material, the comparing device to determine a key assigned to the entered information, to compare the key determined in this way with the stored key and to emit an output signal which indicates whether or not the key determined based on the entered information matches the

stored key.

The invention may also provide for the chip to hold information identifying one or more users and the decrypting device or encrypting device only to be activated when information stored for identifying a user is entered via an input device. The relevant information may be, for example, a password, but also, for example, a fingerprint, an image of the retina, a speech sample for speech recognition, and the like.

The invention may also provide for the code for decrypting coded information contained in the identification data to be stored on a central computer.

The invention may also provide for the computer to determine the corresponding key owing to entered or predetermined genetic information and to apply said key to the identification data.

In this context, the computer may function as a mere decrypting server, i.e. the particular data are stored elsewhere, generally decentralized, the key necessary for decrypting not being present at the particular memory locations and decryption only taking place on said central computer, the central computer receiving the encrypted data and sending back the decrypted data. It is also possible to provide for likewise storing the corresponding animal-related data on the central computer. In this case, the key decrypting the identification data substantially serves to prove that there was no manipulation of the assignment of data on the computer to a particular animal or, when using a one-way function or when the complete data have been encrypted, of the complete data. In contrast, communication between computer and user in this variant is not secured against manipulations or is secured by a standard procedure for establishing a secure connection between a server and a user.

The invention may also provide for the central computer to verify, after decrypting, whether predetermined sequences of characters are present in the decrypted text and emit a corresponding output signal to a user.

The invention may also provide for transferring the animal-specific information stored on a data carrier, which is separate from the central computer, and, where appropriate, predetermined genetic information unambiguously identifying the animal or the material to the central computer where they are decrypted.

The invention may also provide for the data carrier containing the data relating to the animal or the material to be installed on a central computer.

The invention may also provide for at least part of the data to be access-protected and for access authorization to be different for different users of the central computer.

The invention may also provide for a proportion of users to be able to access at least part of the stored data only if a predetermined further user, for example the animal owner, is logged on to the central computer at the same time.

The invention may also provide for access to at least part of the stored data only to be possible, once the computer has verified access authorization using the data stored on a chip, in particular on a smartcard. This may be in particular relevant also to the second user who has to be logged on according to the abovementioned embodiment.

The invention may also provide for setting up the computer such that users can write to the stored data relating to the animal or material only together with a

digital signature of the user.

The invention may also provide for using an animal-specific pair of asymmetric keys for exchanging a session key for communication of a user with the central computer.

The invention also provides a method for generating data which are unambiguously and verifiably connected with an individual animal, which comprises:
- creating identification data in the form of an encrypted message which has an unambiguous and predetermined connection with genetic information which unambiguously identifies an animal or the biological material.
- storing the identification data on a data carrier.

The invention may also provide for the identification data to contain an encrypted message which has been encrypted using a key unambiguously assigned to the individual animal.

The invention may also provide for the encrypted message to contain the value of a one-way function (hash), which value is obtained when applying said one-way function to further data which are stored on the data carrier and which relate to the animal to be identified or the biological material to be identified.

The invention may also provide for the identification data to comprise a message encrypted by a code which is generated in a predetermined unambiguous manner on the basis of a sequence of digits which has been unambiguously assigned to genetic information unambiguously identifying the animal or the material.

The invention may also provide for the key to be a symmetric key.

The invention may also provide for the information to have been encrypted on the basis of an asymmetric pair of keys, with the public key at least in part having a predetermined connection with the genetic information.

5

The invention also provides a chip carrier for identifying animals, which is set up for communication between a chip on the chip carrier and a computer via an interface, for example a reading device, in

10 particular a smartcard, characterized in that the chip holds a key which has an unambiguous and predetermined connection with genetic information specific for the individual animal.

15 The invention may also provide for the chip to have a processor for decrypting messages using the stored key.

The invention may also provide for the chip to contain an interface for entering digitized genetic information

20 and a comparing device for verifying the assignment of the stored code to entered digitized genetic information.

The invention also provides a computer system for

25 carrying out a method as described hereinbefore, which has a central computer having a data carrier which holds identification data which have an unambiguous and predetermined connection with genetic information unambiguously identifying an animal or the biological

30 material.

Advantageously, the method according to the invention makes use of the genetic information of the animals or the biological material for identification and for

35 proving the pedigree. The genetic information is determined, for example, from a blood sample or tissue sample of the animals or from their egg cells or sperm cells using known methods. The root of a hair, for example, is sufficient as a tissue sample. Carriers of

the genetic information are ribonucleic acids (RNA) which represent the substance material of the genes and which are capable of identical duplication. The genetic information may be summarized or else standardized in various ways. To explain particular properties, it is possible to use the genes coded [sic] therefor or genetic markers. In order to ensure access to the genetic information, said information is stored in the form of reference datasets on a storage medium. In order to identify an animal or to prove or verify the pedigree of animals or of biological material, the reference datasets are retrieved from the storage medium and compared with data already available. Before being able to access the reference dataset, the user first has to prove his authorization. This can be done, for example, by entering a password, a name or a PIN. Moreover, the authorization may also be stored on a smartcard, for example. The user may only retrieve the reference dataset for which he can prove authorization. All other reference datasets on the storage medium are not accessible to him. An example of this type of user may be the owner of an animal. He may also pass on his authorization to a third party. In this way it is possible, for example, for the buyer of an animal, to quickly and simply verify whether the data provided by the seller belong to the animal offered for sale. In this case, a time limit is imposed on the authorization for the potential buyer. When missing animals are found, it is possible to verify whether the found animal is the one which is being looked for. In both cases, cell samples may be taken from the animal in order to determine a certain amount of genetic information therefrom. Comparison between the determined information and the reference datasets provides the identity of the animal. In addition, the pedigree of the animals may be determined with the aid of genetic information. For breeding, sperm cells or egg cells are frequently taken from animals and stored appropriately. The gametes are stored in suitable

containers and are available, if needed. When purchasing such gametes, the buyer can determine the pedigree of the gametes by taking a sample and comparing the data determined from the sample with a

5   reference dataset. In this way it is also possible to determine suitable mating suggestions for an optimal breeding result.

There is no danger of manipulation of the reference

10   data in this method, since only authorized persons can retrieve the data. In addition, only a central location may be allowed to modify the reference data so that even authorized persons cannot modify the data. The contents of the reference dataset provide a genetic

15   fingerprint of the relevant animal, organism or biological material. Said fingerprint permits unambiguous identification and can be verified by any laboratory.

20   Biological material from animals or organisms may be stored for storage or handling in suitable containers which are provided with a storage medium for the genetic information of the biological material. To verify the contents, the genetic information determined

25   from a sample of the biological material is compared with the stored data.

According to an advantageous embodiment of the invention, the reference datasets additionally hold

30   characteristics or properties of the animals or the biological material. In this way, a direct link is created between the general characteristics and properties of the relevant animal and the genetic information which is contained in the reference data

35   and which identifies the animal unambiguously ("genetic fingerprint"). The general characteristics and properties may be, for example, specific skills of the animal, the owner, ancestors and descendants, prizes or awards, value declarations, information about general

and specific skills, training, genetic diseases, other diseases, vaccinations or dates of veterinary visits. Examining the reference dataset therefore not only permits the obtaining of knowledge about the abstract
5 genetic information, but also facilitates the retrieval of characteristic data of the animal or of the biological material. In this way, it is also possible to study, evaluate or show the connection between particular genetic information and characteristic
10 features of the animal or of the biological material.

According to another advantageous embodiment of the invention, the characteristics or properties deducible from the genetic information are determined and stored
15 in the reference dataset. The characteristics or properties of the animal may be not only those which have been determined in a study or through observation over a relatively long period or which are based on historical values, but also those which result directly
20 from the genetic information. If the genetic information is present in the form of a reference dataset on a storage medium, it is possible to take advantage of rules already known or else of the latest findings in order to present the characteristics
25 resulting from the genetic information in a quick and simple manner.

According to another advantageous embodiment of the invention, the reference datasets hold photographic
30 pictures. These may be in particular ordinary photographic pictures showing the overall appearance of the animal or else results of visualizing diagnostic methods (e.g. ultrasound examination, X-ray examination, endoscopy, computed tomography), which are
35 used to record the physical state of the animal.

According to another advantageous embodiment of the invention, the biological material is embryos, sperm cells or egg cells from animals. These are, after

having been taken from the relevant animal, filled into suitable containers and stored at low temperature. The containers may carry labeling or electronic data carriers, for example microchips or so-called smart

5   labels, which contain the data essential for the contents of the container. Smart labels are very thin storage units having an interface for input and output which works like a transponder. These smart labels can have the same thickness as a sheet of paper and

10   therefore may be used as "electronic tags" instead of paper tags.

Accessing the reference data makes it possible to verify the data given on the containers, in particular

15   when a sample is taken from the sperm cells or egg cells and the genetic information is determined therefrom.

According to another advantageous embodiment of the

20   invention, the biological material is blood samples or tissue samples from animals, cells from cell cultures or microorganisms. These may be stored, for example, for the purpose of testing or studying. In this case, verification of the sample is possible at any time.

25

According to another advantageous embodiment of the invention, the reference datasets are stored at a central location. This central location manages and monitors the data so that they cannot be manipulated or

30   falsified by third parties. Authorized persons can access the stored data at the central location. The central location may also issue the relevant authorizations.

35   According to another advantageous embodiment of the invention, the reference datasets are encrypted at the central location. This makes it more difficult for unauthorized persons to access the data and prevents corresponding manipulation of the data. Thus it is

possible, for example, to provide a public key and a private key for encrypting and decrypting the data. By retrieving the reference data, the user adds his signature to the dataset contents, comparable to a

5   digital signature.

According to another advantageous embodiment of the invention, the key used is the particular genetic information or the key is based on the particular

10   genetic information. Thus it is possible, for example, to compute the base number determined from the sample of the animal with a control number only known at the central location and to use said base number as a private key.

15

According to another advantageous embodiment of the invention, the authorization for retrieving a reference dataset is stored in particular on a smartcard. In order to retrieve the reference dataset, the smartcard

20   has to be inserted into a reading device provided for this purpose. The reference data are released, only after the authorization has been verified and recognized. The card user receives suitable software with the aid of which he is able to access the

25   reference data on his computer. A data network offers the possibility of accessing the reference data online. For this purpose a suitable data connection between the central location and the user is required. Instead of a smartcard it is also possible to provide a different

30   carrier of an isolated chip having an interface for communicating with a computer, for example in the form of a bracelet, a key ring or another object which the user may wear on his body; the interface need not necessarily be electronic, but may, where appropriate,

35   also work optically. The term "chip" in the context of this application ought to mean not only electronic semiconductor components having a memory function and a built-in microprocessor, but also memory chips having solely memory function or other memory devices of

similar size - and/or logic units, for example holographic memory devices or the like. Accordingly, a "smartcard" or a "chip carrier" in the context of this application means also a carrier or card which carries a chip in accordance with this application. The chip carrier generally has similar or smaller dimensions than a smartcard.

According to another advantageous embodiment of the invention, a password, name or PIN is entered for proof of authorization when retrieving a reference dataset.

According to another advantageous embodiment of the invention, the genetic information of the reference datasets is used to determine mating suggestions for breedings. For this purpose, it is possible to select from the reference datasets suitable male and female animals in order to achieve the desired breeding result. Data in the form of reference datasets make the selection from among a relatively large total number of animals easier.

According to another advantageous embodiment of the invention, the storage medium containing the reference data and, where appropriate, access authorizations is integrated into an identity tag which is worn by the animal. This makes assigning the animals easier.

According to another advantageous embodiment of the invention, an output device linked to the storage medium displays the genetic information of the reference datasets in the form of a histogram. This diagram makes it possible to visually register the genetic information quickly and simply and to compare said information with that of other animals.

In the following, some aspects of the invention are explained in more detail.

A problem occurring frequently in connection with the identification of animals is the exchange of documents referring to the animal, and it is not easily possible to assign unambiguously the contents of the documents
to the animal. Safe assigning of the key to the particular animal or to authorized persons is a great problem for protecting identifying information against falsifications. To this end, the invention provides a method which integrates safe individualizing
information (e.g. genetic fingerprint) into the production of the keys, either into the keys per se or into certificates which assign the keys certified by a certification authority to particular persons or animals.

According to a preferred embodiment, the invention provides as a solution to this problem that the animal-related data on the data carrier have either themselves been encrypted using a key unambiguously connected with genetic information unambiguously identifying the animal or that verifying information which irreversibly and unambiguously identifies further information, which pedigreeally has been stored and need not be encrypted, is encrypted using such a code. Such verifying information can be generated by so-called one-way functions, also called hash functions. If, after encrypting, said further unencrypted information on the data carrier is manipulated, this can be detected by comparing the coded and stored value of the one-way function with the value which is obtained when applying the one-way function to the data actually stored on the data carrier. If the two values do not match, then the data have been modified or the wrong key was used for decrypting.

Genetic information which unambiguously identifies an animal or an organism can be obtained, for example, using the so-called microsatellite method. This method makes use of the fact that in particular regions of the

genome a particular sequence of bases, for example CA, is repeated with an individually different number of repeats. These regions are flanked by stable genomic regions which serve as target sequence for the binding
5   of primers in a polymerase chain reaction (PCR). If the number of these repeats is determined in a sufficiently large number of appropriate genomic regions, the total amount of these repeats is specific for the individual animal or the individual organism.
10

If then a particular sequence of the genomic regions, in which these repeats are determined, is fixed and numbers corresponding to the number of these repeats are arranged according to this sequence, then a
15   sequence of digits is obtained therefrom which is likewise specific for the specific individual.

Another method for presenting individual genetic information makes use of polymorphisms at individual
20   nucleotide positions of the genome. The SNP (single nucleotide polymorphism) method provides a dataset in which for each of the studied genome positions the statement 1 (= result 1, e.g. corresponds to the population value) or 0 (= result 2, e.g. deviating
25   value) is obtained. The results of the study in their entirety produce a binary number (e.g.011100010100001111101010). For safe individualization approx. 40 genomic sites have to be studied. At present there are neither for humans nor
30   for other organisms any defined standards denoting the positions to be studied. To obtain SNP information, various methods are available which are increasingly automated in the form of DNA chips which facilitates high sample throughput. Examples of different
35   approaches are the fixing of oligonucleotides specifying a specific position on chips. Another technique provides for distinguishing the polymorphic PCR products by their molecular weight (Internationales Technologieforum 99, 23/24 June 1999, ICM

Internationales Congress Center, Neue Messe Munich).

Most encryption algorithms start out from a random
number based on which the key is then generated. If
5   this random number is then replaced by a sequence of
digits which is specific for the individual and which
has been obtained from the genetic information in the
above-described manner an encrypting code specific for
the relevant individual is obtained. Generally it is
10   possible to use for generating the key any digitized,
preferably   genetic   information   unambiguously
identifying the animal.

According to the invention, it is possible to verify
15   whether the animal in question corresponds to the
stored data, by taking a sample from the animal,
determining the appropriate genetic information and
verifying whether the key corresponding to this
information is the key for decrypting the coded data.
20   If it is impossible to decrypt the encrypted
information or if the stored value of a one-way
function is different from the remaining data, as
previously described, due to applying the wrong key,
then manipulation of the data or an exchange of the
25   animal must be suspected. In this way, it can be
excluded that the animal to which the data refer has
been exchanged.

Another problem is that the stored data can be
30   falsified on the data carrier or during transport via
the Internet. This risk can be diminished by
restricting and controlling the group of persons who
have access to the key or to the assigning of the key
to genetic information. Another way to proceed is to
35   send the encrypted part of the data to a trustworthy
central location for decrypting, which location re-
transmits the decrypted result without releasing the
key required for decryption and, where appropriate,
verifies the authenticity of the data and/or the

assigning of the animal to the stored data.

This method, however, is complicated and offers no guarantee that the information exchanged between the trustworthy location and a user remains unmodified. Furthermore, it is important in this procedure that, if possible, the key is not revealed even to the owner of the animal, since otherwise there is the danger of falsifying the data using the correct key. It would also be desirable for an owner to be able to verify directly, using genetic information, whether the animal in question corresponds to the stored data.

It is possible to circumvent these problems by using an asymmetric pair of keys, the public key being unambiguously connected with the genetic information which identifies the animal and which may be known to the owner or may be directly verified by said owner, while the private key used for encrypting the data is only known to the person or the location or is only available to said person or at said location, that has written the data on the data carrier or is authorized to do so.

Asymmetric keys are generally known in data technology and form, i.a. the basis for the digital signature. Regarding details relevant to the encryption of data and regarding other aspects of data security, in particular one-way functions or hash functions, reference is made to M. Raepple, "Sicherheitskonzepte für das Internet", Heidelberg 1998 or to RSA Laboratories "Answers to Frequently Asked Questions About Today's Cryptography", Version 3.0.

The following describes an example of how an asymmetric RSA code can be generated based on genetic information.

An RSA code can be generated as follows:
- take 2 large prime numbers p and q,

- form their product n = p.q,
- choose a number e which is less than n and not divisible by p-1 and q-1,
- find a number d such that (e.d)-1 is divisible by
5   (p-1).(q-1).

The value pair (n, e) forms the public key and the pair (n, d) forms the private key. The factors p and q are deleted or securely stored together with the private
10   key.

To encode a message m using the public key, the power of m is modularly raised according to the formula $c = m^e$ mod n. To decode, the power of the coded message c is
15   raised on the basis of the private key and according to the formula c^d mod n. The structure of the RSA key is precisely such that consequently the original message m is exactly reproduced. Conversely it is also possible to encode using the private key according to the same
20   formulae and then decode using the public key.

To generate an animal-specific pair of keys, it is possible in the RSA algorithm, for example, to equate the number determined from the genetic information with
25   the number e, which, after factorization of e, results in prime numbers p and q for which p-1 and q-1 are not divisible by e. According to the RSA algorithm, the number d is then determined so that the public key contains as a parameter the number e which corresponds
30   to the abovementioned genetic information. If the private key which is only accessible to the owner of the animal, to a trustworthy authority or the like is then used to encrypt information within the dataset, for example the result of a hash function, a successful
35   decryption using the public key may then not only verify that the stored information is indeed related to the animal in question (which, in the present example, is possible by comparing e with genetic information obtained directly from the animal), but may also verify

the person who carried out the encryption, just like a digital signature.

It should be taken into account in this connection that the second parameter of the public and private keys, n, is not unambiguously defined in the abovementioned example. Accordingly, it is possible to generate a plurality of keys which are, in the abovementioned sense, specific for the animal, but belong to different persons. This makes it possible for different persons, whose authenticity can be directly verified, to be able to write animal-related data to the data carrier.

Another possibility to facilitate authentication of the person who has written data to the data carrier is to encrypt the message encoded by the "animal-specific code" again by a code specific for the particular user, or to have the relevant user in a conventional manner digitally signing a text, which he has generated, by him, for example, calculating the value of a hash function from the generated text and encrypting this value using his private key out of an asymmetric pair of keys, this coded value then being added to the dataset.

In order to further increase verification and security of the key used, it is possible to provide for implementing the key required for decryption on a smartcard. In this context, it is possible to provide either for a computer used for decryption to access the key securely stored on the smartcard and to use said key for decryption, or, preferably, for the smartcard itself to contain a processor for decrypting messages so that an encrypted text is entered into the card and an uncoded text is printed out, while the stored code itself does not get outside. The smartcard may also be provided for storing the private key of a user and, preferably, may have a processer for encrypting messages using the private key.

Assigning the smartcard to a particular animal may be carried out in various ways.

5   The simplest possibility is choosing the public key, for example as previously explained, in such a way that genetic information specific for the animal is part of the public key, for example such that this information forms the parameter e. In this context, the public key
10 may be printed, in the simplest case, on the smartcard or may be retrieved from the smartcard memory by a simple output operation.

    If the public key is not to become known to everybody,
15 then it is also possible to provide for storing an assigning instruction between the genetic information and the public key on the chip of the smartcard and for the smartcard to be set up in such a way that digitized genetic information obtained from the actual animal can
20 be entered. A processor in the smartcard then calculates the key from the entered digitized information, according to the assigning instruction, and compares said key with the stored key. If there is a match, the processor states that the entered
25 information corresponds to the stored key, and it states that the smartcard does not correspond to the relevant animal, if there is no match between the stored key and the key determined by the processor. The smartcard preferably contains further information,
30 retrievable as uncoded text, about which methods have been used to obtain the genetic information on which the key stored on the smartcard is based, and about which method is used to digitize the obtained information. A user to whom the appropriate genetic
35 information relevant to the animal in question is available therefore does not require a certification authority or the like in order to detect whether a particular code or a particular smartcard has indeed been assigned to a particular animal. He may detect

this by himself using the genetic information obtained from the animal and the information stored on the smartcard. This also gets rid of all problems which, in connection with the digital signature, derive from the communication between a user and a certification authority. The physical link between keys and animal-identifying data on the smartcard prevents manipulation of the communication and of the components required for secure data transport.

The above-described method can be used for setting up a system for the certification and verification of animals on an electronic basis. The data relevant to the animal, for example date of birth, ownership data, vaccination data, etc., are stored at a certification authority on a central computer which is accessible in the usual way for privileged users and on which, where appropriate, part of the stored data is publicly accessible. The appropriate data have either been encrypted using the private key of an animal-specific asymmetric pair of keys, i.e. a code which is based on genetic information about a particular animal in the manner mentioned above, or the value of a one-way function which results from this one-way function being applied to the appropriate dataset has been added to each dataset, encrypted by said animal-specific private key. In both cases, it is possible for a user reading the appropriate data or receiving them via the Internet to verify that said data are genuine and that they derive from a particular person.

The owner of the animal receives an animal-specific smartcard which holds the animal-specific asymmetric key, i.e. the private as well as the public key. The smartcard simultaneously serves as an animal identity card which contains a certificate from the certification authority. The certificate contains the name of the animal, a continuous serial number, the name of the issuing authority, the name of the

applicant, the name of the place which has obtained the genetic information on which the coding is based ("genetic fingerprint"), the method which obtained this information, the genetic information itself and a
5   validity period and also, where appropriate, information about the public key and/or about the encryption method. This certificate is readable from the chip as uncoded text or using a public key of the certification authority. The certificate may also be
10 printed on the smartcard, if desired.

In order to obtain access to the data stored at the certification authority, the genetic information and public key are read out from the smartcard via a
15 reading device and transmitted to the certification authority. Using the genetic information, the computer of the certification authority determines data related to which animal are to be released. Using the public key, the computer verifies whether the user logged on
20 is authorized to read the data. It is also possible to transmit other data instead of the genetic information, for example a serial number which refers to the relevant animal. Likewise it is possible to provide for additional or alternative devices for blocking access,
25 for example passwords.

The owner receives an access authorization for those parts of the data stored on the central computer which are owner-related, for example place of rearing,
30 nutritional data, and the like. For other data, for example date of birth, place of pedigree, and the like, the owner only receives a restricted access authorization, although he possesses the appropriate private key. Generally, he will be allowed to read
35 these data but not to modify or to delete them. Access authorization can be set up in a conventional manner by issuing read and write privileges on the central computer and/or by a conventional password. Other access control mechanisms, for example speech

recognition or the use of physical characteristics of the relevant person (fingerprint, iris scan, etc) may also be used. Another possibility of access control, which may be provided for, is to allow data access only

5 when the user deposits a digital signature, i.e. a message encoded by a private key which has been assigned to the user by a certification authority which can be the certification authority for the animal data or else a certification authority according to the

10 digital signature act.

It is also possible to provide for a single smartcard (master card) facilitating access to data relating to a plurality of animals, for example for breeders or

15 organizations, this master card preferably containing only the particular public keys but not the private keys so that the owner of this master card can read all data relating to the various animals but cannot modify them without the animal-specific card described

20 hereinbefore.

The persons running the certification authority likewise possess the private and the public animal-specific codes and have full access authorization for

25 all parts of the data.

It is possible for the owner (or the certification authority) to facilitate third-party access to the data by allowing said third parties to read the data, either

30 for a limited time or permanently, for example by issuing a password and providing said third parties with the public animal-specific key. It is further possible to allow particular users, for example veterinarians, to modify or rewrite particular data,

35 for example vaccination data, examination data, etc., said users then digitally signing, for example by encrypting the value of an appropriate one-way function, the data which they modified or rewrote using a private key specific for them. If these data are

modified, the certification authority generates a second signature in the form of the coded value of a one-way function using the animal-specific private key, in order to confirm the authenticity of the assigning of the written data to the corresponding animal.

It is, however, also possible to provide for a third party being able to access the data and to read and/or modify them only when using simultaneously the animal-specific smartcard of the owner for authorization by inserting said card into an appropriate reading device. In this case, he can access the data stored at the certification authority only if this smartcard has been handed to him and if the owner has thus authorized him.

The example of a veterinarian who has writing authorization for data at the certification authority serves to further illustrate third-party access.

The veterinarian has a private and a public key available which have been assigned to him by the certification authority and or [sic] according to the digital signature act. A file ("register sheet") for treatment data has been created in the electronic register created by the certification authority. The veterinarian receives reading authorization for the parentage data such as date of birth, pedigree datum, etc., and an access authorization for writing and reading vaccination data and for writing treatment data, the privilege of reading treatment data which are not connected with his work possibly being restricted.

During a treatment session, the animal owner hands the animal-specific smartcard assigned to the animal over to the veterinarian who establishes a link to the certification authority with the aid of this card. Reading the information of the certificate and transmitting data stored on the animal-specific card, such as the stored and animal-specific public key and a

password, to the certification authority, opens access to the stored data at the certification authority, which relate to the actual animal. To read or write data, the veterinarian has to personally identify himself once more. This can be done by transmitting data of a smartcard assigned to the veterinarian or by transmitting data, which are securely stored on the smartcard reading device or on the computer of the veterinarian, automatically to the central location. The usual techniques for a secure link may be used for communication between the veterinarian and the certification authority. It is, for example, possible to exchange with the aid of an asymmetric pair of keys a symmetric session key which has been specifically generated for the session and which is used to encrypt the entire communication between the veterinarian and the certification authority during the session.

Once both the authorization relevant to the animal and the authorization of the veterinarian have taken place, the veterinarian may read or, if permitted, modify the data accessible to him in the register of the certification authority. The veterinarian adds a digital signature to the data modified or rewritten by him.

A communication is also possible in the reverse direction, for example for transmitting data about illnesses. In this context, the appropriate message is encrypted either using the animal-specific private key or the private key of the veterinarian or the public key of the recipient. Alternatively, the message is sent uncoded and, to verify authenticity, a signature, for example the value of a one-way function applied to the message, encrypted using the animal-specific private key or the private key of the veterinarian, is generated and attached to the message.

The above-described method may be used, for example,

for identifying animals at breeding shows. To register the animal, the animal owner transmits the genetic information which identifies the animal and which is the basis of the public animal-specific key, as explained hereinbefore, and also the public animal-specific key given on the smartcard or other information assigning the smartcard to the genetic information. When arriving at the breeding show, the animal is identified using the transmitted genetic information. The certificate, stored on the smartcard or printed, is used as a basis for verifying that the public key given belongs indeed to the genetic information given so that the smartcard is authentically assigned to the animal presented. The smartcard verified in this way can then be used to access the data at the certification authority. If the data at the certification authority can be decrypted using the key stored on the smartcard, then it has been established that the animal presented corresponds to the data stored at the certification authority.

It is possible to proceed in a similar way also for business transactions relating to the animal, for example for animal sales. In this case too, the public key is transmitted together with the genetic information identifying the animal. Instead of the public key, it is also possible to transmit other information which produces unambiguous assigning of a smartcard to be present [sic] to the transmitted genetic information. As long as the smartcard verifies the assigning of the stored data, in particular of the stored code, to the genetic information automatically, giving the genetic information alone is sufficient for authentication of the card.

Various modifications of the above-described procedure are possible. It is possible, for example, to use other encryption methods. Access authorizations, in particular reading or writing privileges, may be

organized differently.

Information relevant to obtaining the genetic information, the assigning of this information to a public key, etc. need not be stored on a smartcard, but may also be communicated in a different manner.

The method may be developed into an Internet marketplace, for example for electronic animal trade or electronic animal auctions. In this context, particular information of the reference datasets or, more generally, of the data which are stored at the certification authority and are relevant to the registered animals and/or materials, is made available via search functions. The marketplace may be open, it being possible to protect data transmission by standard methods. Alternatively, access to the information in general or else only to particular information may be restricted to authorized users.

In the context of building up a genetic certification authority, specific genetic information of the reference datasets may be issued as electronic or written certificates for particular animals or materials, in particular as certificate for other properties and/or characteristics.

Finally, the method according to the invention may be used for building up a standardized animal database for which no longer the genetic information (the "genetic fingerprint") forms the animal-identifying data, but rather the key assigned to this information. The methods which are at present used for producing a "genetic fingerprint", are different so that one and the same animal may correspond to a plurality of "genetic fingerprints", depending on the method used. Accordingly, it is at present difficult, to screen various databases for data relating to the same animal by using the genetic information. Within the scope of

the invention, the method of obtaining the genetic
fingerprint is unimportant as long as only a single
individually assigned key (or other digital
information) is assigned to each animal; the principal
5   search criterion is the animal-specific code or key. A
certificate naming the method, which is used for
determining the genetic fingerprint, and the assigned
key links the key and the specific genetic information,
this certificate always being available together with
10   the key and either being stored together with said key
or being retrievable from a server at any time.

The characteristics of the invention which are
disclosed in the above description and in the claims
15   may be important both alone and in any combination for
the realization of the invention in its various
embodiments.

Dr. Eberhard Manz

GM 2238 PCT

_____

Patent Claims
_____

1. Method for proving the pedigree and/or for the identification of animals or of biological material from animals and organisms, which comprises the following steps:
   - storing on a data carrier identification data in the form of an encrypted message which has an unambiguous and predetermined connection with genetic information unambiguously identifying an animal or the biological material,
   - verifying the identification data with respect to whether said data have the predetermined connection with the genetic information.

2. Method according to Claim 1, [lacuna] that the genetic information of one or more animals or of biological material from one or more animals or organisms is determined and is stored as reference datasets on a storage medium.

3. Method according to Claim 1 or 2, characterized in that the data carrier holds further data which have been assigned to the identification data and which relate to the animal to be identified or the biological material to be identified.

4. Method according to Claim [sic] 1 to 3, characterized in that the identification data contain an encrypted message which has been encrypted using a code unambiguously assigned to the individual animal or material.

5. Method according to Claim 4, characterized in that the encrypted message contains the value of a one-way function (hash), which value is obtained when applying said one-way function to further data which are stored on the data carrier and which relate to the animal to be identified or the biological material to be identified.

6. Method according to one [lacuna] Claims 1 to 5, characterized in that an encrypted message comprises genetic information unambiguously identifying the animal or the material.

7. Method according to one of Claims 3 to 6, characterized in that the identification data comprise encrypted data which relate to the storage location and/or the contents of further data which relate to the animal assigned to the identification data.

8. Method according to one of Claims 4 to 7, characterized in that the identification data comprise a message encrypted by a code which is generated in a predetermined unambiguous manner on the basis of a sequence of digits which has been unambiguously assigned to genetic information unambiguously identifying the animal or the material.

9. Method according to Claim 8, characterized in that the sequence of digits forms at least part of the code.

10. Method according to Claim 8 or 9, characterized in that the key is a symmetric key.

11. Method according to Claim 8 or 9, characterized in

that the message has been encrypted on the basis of the private key of an asymmetric pair of keys, with the public key at least in part having a predetermined connection with the genetic information identifying the animal or the material.

5

12. Method according to Claim 11, [lacuna] that the public key comprises a part specific for the animal or the material and a user-specific part.

10

13. Method according to one of Claims 8 to 12, characterized in that the identification data are additionally encrypted using a user-specific key.

15 14. Method according to one of Claims 8 to 13, characterized in that the data on the data carrier, which have been assigned to the identification data, have at least in part been encrypted by a code which is different than the code used for encrypting the

20 identification data.

15. Method according to one of Claims 8 to 14, characterized in that the key for decrypting the message contained in the identification data is

25 stored on a carrier of a chip for communicating with a data processing system via an interface, in particular on a smartcard.

16. Method according to Claim 15, characterized in that

30 the chip has a device for decrypting messages.

17. Method according to Claim 15 or 16, characterized in that the key encoding the message of the identification data is an asymmetric key, the

35 corresponding private key is stored on the chip and the chip has a device for encrypting messages using

the private key.

18. Method according to one of Claims 15 to 17, characterized in that the chip contains an interface for entering digitized genetic information and a device for verifying the assignment of the stored code to entered digitized genetic information.

19. Method according to Claims 18, characterized in that the comparing device compares the entered digitized genetic information with a stored value for this information and emits an output signal which indicates whether or not there is a match.

20. Method according to Claim 18, characterized in that, based on the entered digitized genetic information and a stored assignment to the stored key of digitized genetic information unambiguously identifying the animal or the material, the comparing device determines a key assigned to the entered information, compares the key determined in this way with the stored key and releases an output signal which indicates whether or not the key determined based on the input matches the stored key.

21. Method according to one of Claims 15 to 20, characterized in that the chip holds information identifying one or more users and the decrypting device or encrypting device is only activated when information stored for identifying a user is entered via an input device.

22. Method according to one of Claims 8 to 21, characterized in that the code for decrypting coded information contained in the identification data is stored on a central computer.

23. Method according to Claim 22, characterized in that the computer determines the corresponding key owing to entered or predetermined genetic information and applies said key to the identification data.

24. Method according to Claim 23, characterized in that, after decrypting, the central computer verifies whether predetermined sequences of characters are present in the decrypted text and releases a corresponding output signal to a user.

25. Method according to Claim 23 or 24, characterized and that the information stored on the data carrier and, where appropriate, predetermined genetic information unambiguously identifying the animal or the material are transferred to the central computer.

26. Method according to one of Claims 1 to 24, characterized in that the data carrier containing the data related to the animal or the material is stored on a central computer.

27. Method according to Claim 26, characterized in that at least in part the data are access-protected and that access authorization is different for different users of the central computer.

28. Method according to Claim 27, characterized in that a proportion of users can access at least part of the stored data only, if a predetermined further user is logged on to the central computer at the same time.

29. Method according to one of Claims 26 to 28, characterized in that access to at least part of the stored data is only possible, if the computer has

verified access authorization using the data stored on a chip, in particular on a smartcard.

30. Method according to one of Claims 27 to 29, characterized in that the computer is set up such that users can write to the stored data related to the animal or the material only together with a digital signature of the user.

31. Method according to one of Claims 26 to 30, characterized in that an animal-specific pair of asymmetric keys is used for exchanging a session key for communication of a user with the central computer.

32. Method for generating data which are unambiguously and verifiably connected with an individual animal, which comprises:
   - creating identification data in the form of an encrypted message which has an unambiguous and predetermined connection with genetic information which unambiguously identifies an animal or the biological material.
   - storing the identification data on a data carrier.

33. Method according to Claim 32, characterized in that the identification data contain an encrypted message which has been encrypted using a key unambiguously assigned to the individual animal.

34. Method according to Claim 33, characterized in that the encrypted message contains the value of a one-way function (hash), which value is obtained when applying said one-way function to further data which are stored on the data carrier and which relate to

the animal to be identified or the biological
material to be identified.

35. Method according to one of Claims 32 to 34,
characterized in that the identification data
comprise a message encrypted by a code which is
generated in a predetermined unambiguous manner on
the basis of a sequence of digits which has been
unambiguously assigned to genetic information
unambiguously identifying the animal or the material.

36. Method according to Claim 35, characterized in that
the key is a symmetric key.

37. Method according to Claim 35, characterized in that
the information has been encrypted on the basis of an
asymmetric pair of keys, with the public key at least
in part having a predetermined connection with the
genetic information.

38. Chip carrier for identifying animals, which is set up
for communication between a chip on the chip carrier
and a computer via an interface, in particular a
smartcard, characterized in that the chip holds a key
which has an unambiguous and predetermined connection
with genetic information specific for the individual
animal.

39. Chip carrier according to Claim 38, characterized in
that the chip has a processor for decrypting messages
using the stored key.

40. Smartcard according to one of Claims 38 or 39 [sic],
characterized in that the chip contains an interface
for entering digitized genetic information and a
device for verifying the assignment of the stored

code to entered digitized genetic information.

41. Computer system for carrying out a method according
     to one of Claims 1 to 31, characterized by a central
     computer having a data carrier which holds
     identification data which have an unambiguous and
     predetermined connection with genetic information
     unambiguously identifying an animal or the biological
     material.

Dr. Eberhard Manz

GM 2238 PCT

Abstract

The invention relates to a method for proving the pedigree
and/or for the identification of animals or of biological
material from animals and organisms, which comprises the
following steps:
- storing on a data carrier identification data in the
  form of an encrypted message which has an unambiguous
  and predetermined connection with genetic information
  unambiguously identifying an animal or the biological
  material,
- verifying the identification data with respect to
  whether said data have the predetermined connection
  with the genetic information,

and also to a smartcard and a computer system to be used
for this method and to a method for generating data
assigned to the animal.

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD FOR DETERMINING THE ORIGIN OF AND/OR IDENTIFYING ANIMALS OR BIOLOGICAL MATERIAL, the specification of which (check one)

X   is attached hereto

X   was filed on _____June 30, 1999_____ as Application Serial No. _____PCT/DE99/01937_____ and was amended on
_____ (if applicable).

X   I hereby authorize and request our attorney, Davidson, Davidson & Kappel, LLC. of 485 Seventh Avenue, New York, New York 10018 to insert here in parentheses (Application number _____, filed _____) the filing date and application number of said application when known.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose all information which is known to me to be material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign and/or provisional application(s) for patent or inventor's certificate listed below and have also identified below any foreign and/or provisional application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

PRIOR APPLICATION(S)

			Priority claimed	
198 29 034.9	Germany	30 June 1998	X	
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

PCT/DE99/01937	June 30, 1999	Pending
(Application Serial Number)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial Number)	(Filing Date)	(Status) (patented, pending, abandoned)

And I hereby appoint Clifford M. Davidson, Registration No. 32,728, Leslye B. Davidson, Registration No. 38,854, Cary S. Kappel, Registration No. 36,561, William C. Gehris, Registration No. 38,156, Morey B. Wildes, Registration No. 36,968, Robert J. Paradiso, Registration No. 41,240, Scott L. Appelbaum, Registration No. 41,587, Cynthia R. Moore, Registration No. 46,086, David Knasiak, Registration No. 45,991, Salvatore J. Maiorino, Registration No. 42,830, my attorneys, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith; correspondence address: DAVIDSON, DAVIDSON & KAPPEL, LLC, 485 Seventh Avenue, 14the Floor, New York, New York 10018; Telephone: (212) 736-1940; Fax: (212) 736-2427.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon

Full name of sole or first
Inventor __Dr. Eberhard Manz_____

X Inventor's signature _____
Date __Dec. 19, 2000__
Residence__Heidelberg, Germany DEX__
Citizenship __German__
Post Office Address: __Langgewann 34__
_____D-69121 Heidelberg, Germany__

Full name of second
Inventor, if any_____

Second Inventor's signature _____
Date_____
Residence_____
Citizenship _____
Post Office Address:_____
_____

Full name of third
Inventor, if any _____

Third Inventor's signature _____
Date _____
Residence_____
Citizenship _____
Post Office Address: _____

Full name of joint
Inventor, if any _____

Fourth Inventor's signature _____
Date _____
Residence_____
Citizenship _____
Post Office Address:_____